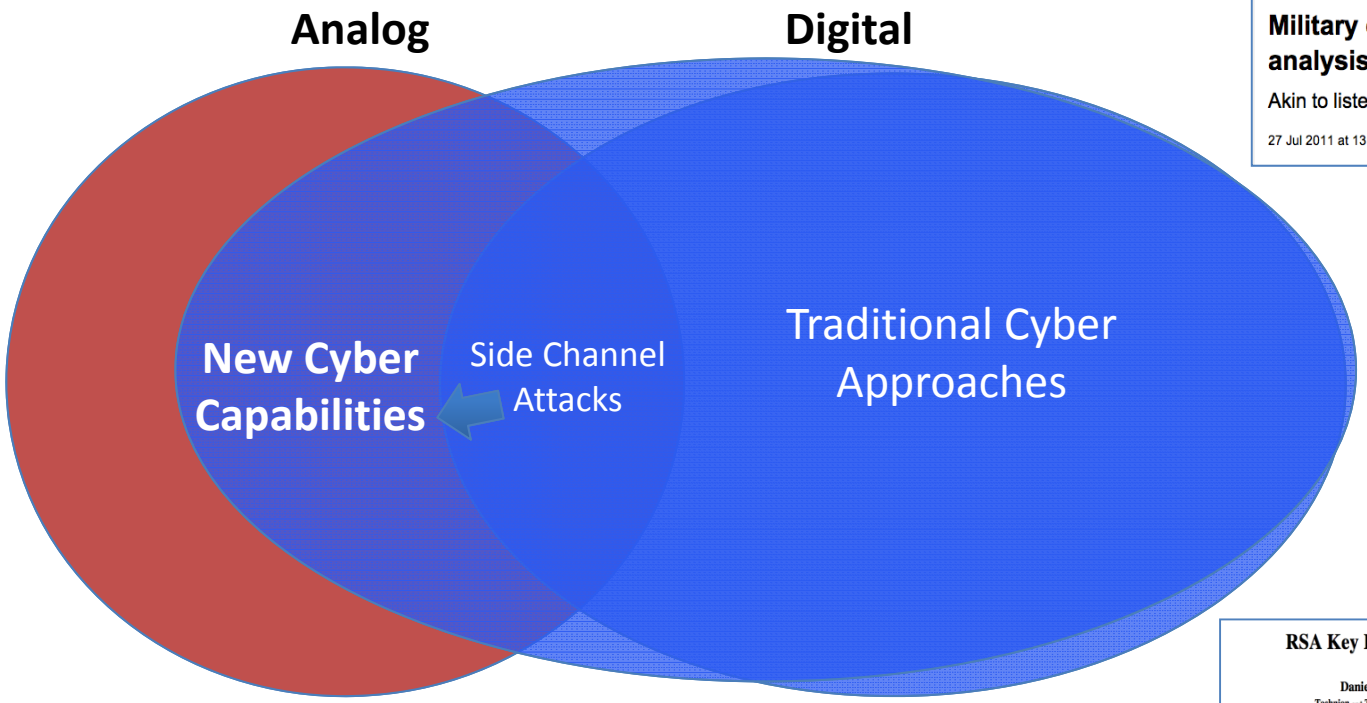
Leveraging the Analog Domain for Security

Angelos D. Keromytis
Program Manager
Information Innovation Office (I2O)

October 1, 2015

Unexplored Opportunities for Cybersecurity at the Intersection of Analog and Digital



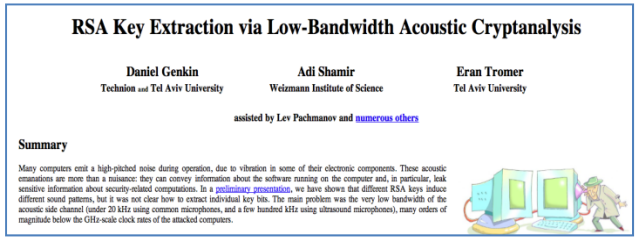

The Register
Biting the hand that feeds IT

DATA CENTER SOFTWARE NETWORKS SECURITY BUSINESS HARDWARE SCIENCE BOOTNOTES

Military chip crypto cracked with power-analysis probe

Akin to listening to safe tumblers, but with 'leccy

27 Jul 2011 at 13:54, John Leyden 117 17 23


RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis

Daniel Genkin, Technion and Tel Aviv University
Adi Shamir, Weizmann Institute of Science
Eran Tromer, Tel Aviv University

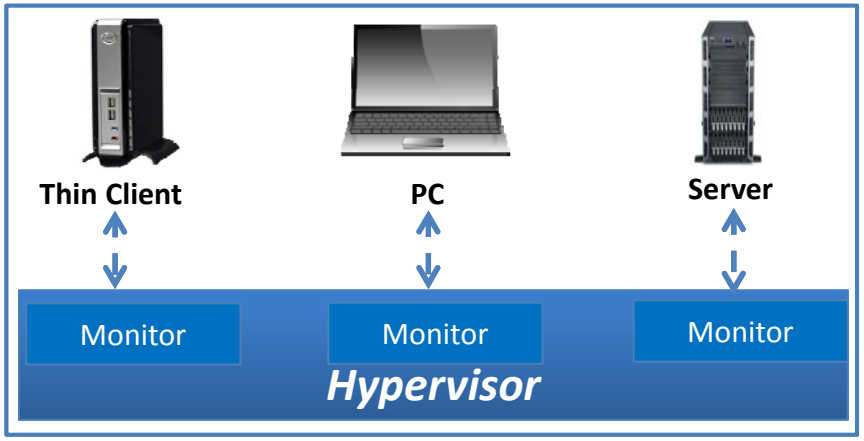
assisted by Lev Pachmanov and numerous others

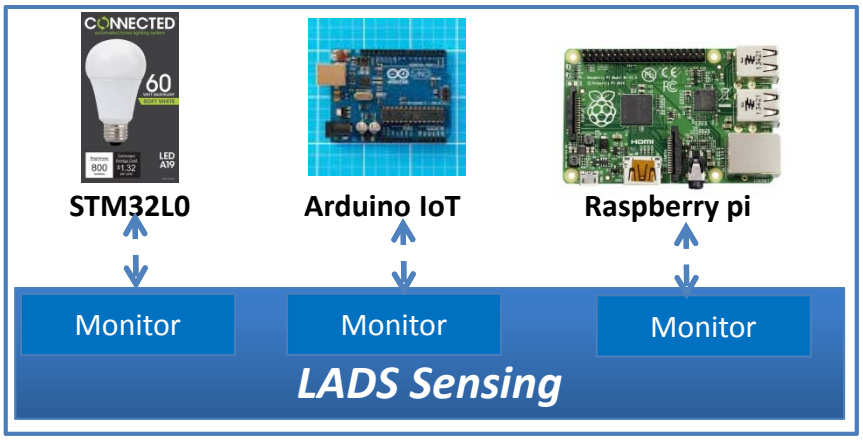
Summary

Many computers emit a high-pitched noise during operation, due to vibration in some of their electronic components. These acoustic emanations are more than a nuisance: they can convey information about the software running on the computer and, in particular, leak sensitive information about security-related computations. In a preliminary presentation, we have shown that different RSA keys induce different sound patterns, but it was not clear how to extract individual key bits. The main problem was the very low bandwidth of the acoustic side channel (under 20 kHz using common microphones, and a few hundred kHz using ultrasound microphones), many orders of magnitude below the GHz-scale clock rates of the attacked computers.

- Analog and digital are generally viewed as distinct areas in cybersecurity
  - Ignoring the analog side simplifies an already hard problem
  - We can usually afford to rely only on digital techniques (i.e., more code/logic)

Using Analog to Protect Low-Resource Devices





Traditional IT:

- Resource-rich environment with numerous existing and new capabilities for cyber defense
- Defenses do not readily translate to low-resource environments

IoT and Embedded:

- Resource, logistic, and physical constraints make it difficult to embed security functionality
- Attack surface is large and easy to exploit
- Single penetration leads to total compromise


NETWORKWORLD Most read:

Researchers exploit ZigBee security flaws that compromise security of smart homes

Network World | Aug 11, 2015 10:54 AM PT


The Register

Security

Compromised Cisco routers spotted bimbling about in the wild

Diseased boxen lassoed in four countries as malicious actors find their way into systems


SECURELIST

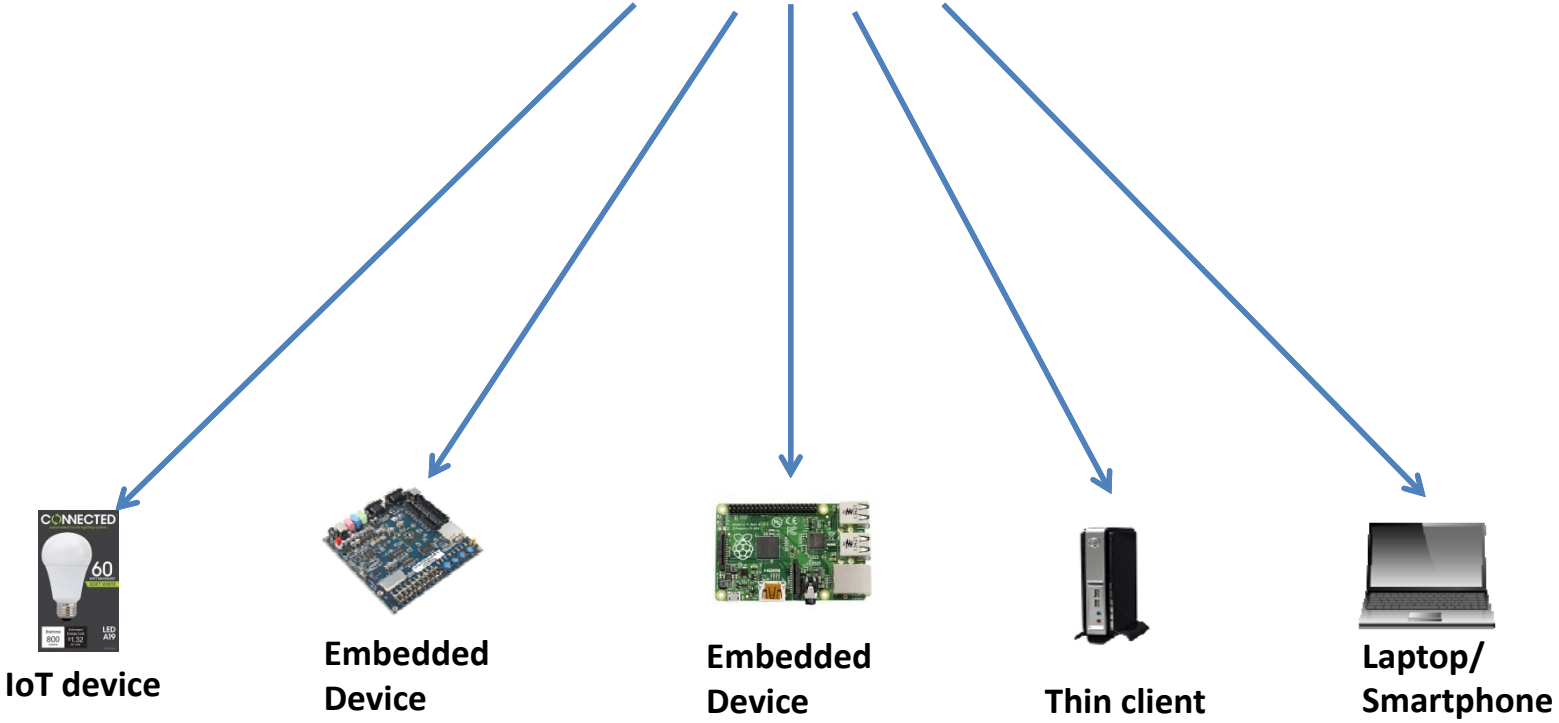
Equation: The Death Star of Malware Galaxy

By GReAT on February 16, 2015. 6:55 pm

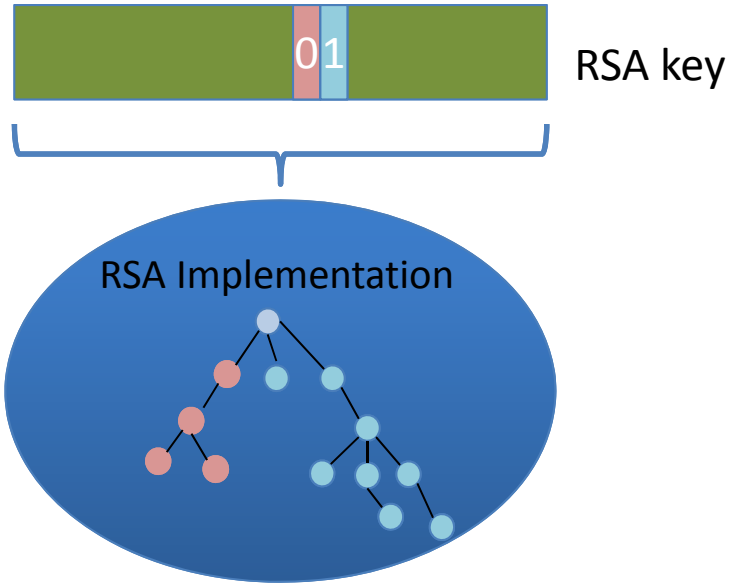
Use the analog domain to enable new classes of defense in low-resource and embedded devices (e.g., IoT)

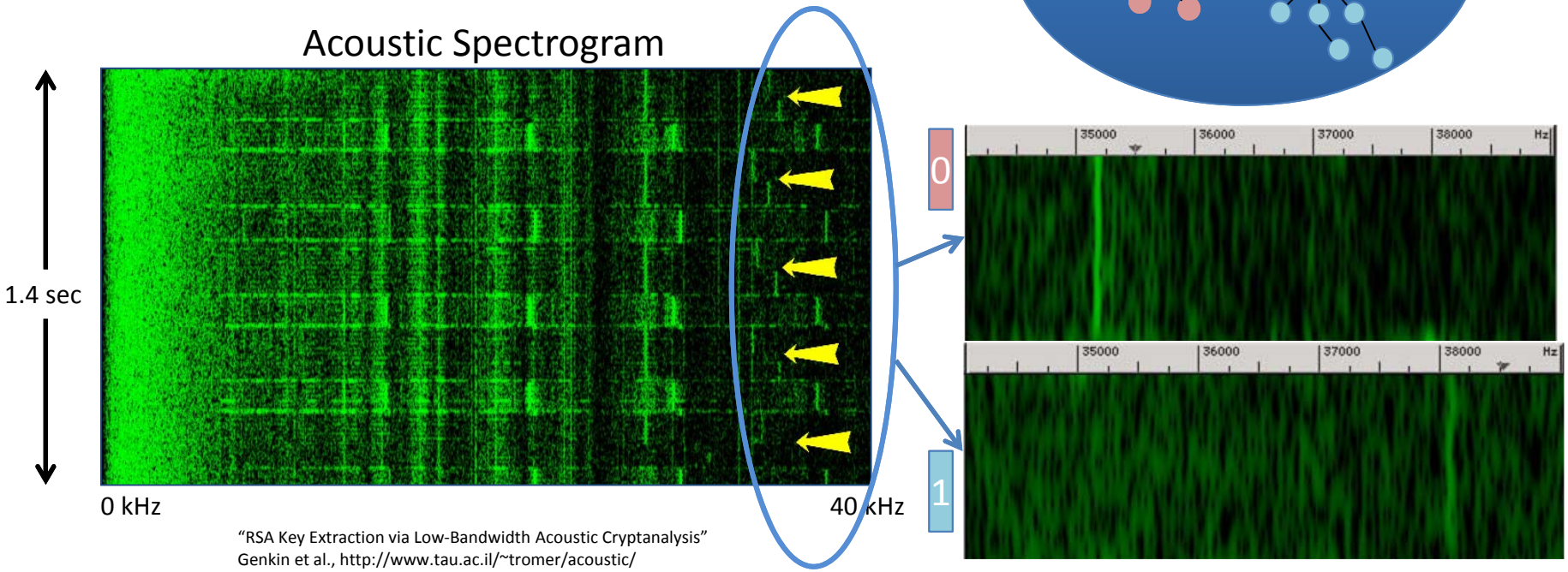
LADS Program Structure

TA1: Protecting Embedded and Mission-Specific Devices (EMSDs) via Analog Sensing



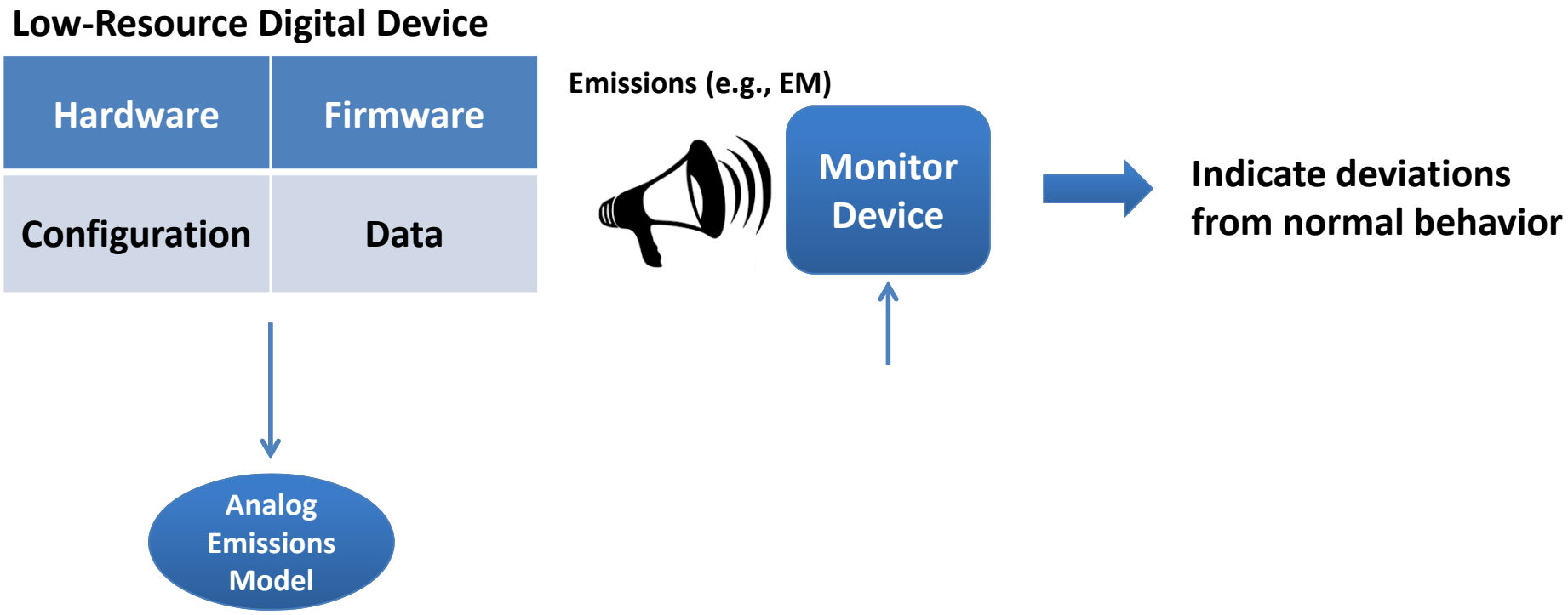
Example: Extract Cryptographic Keys by Tracking Code Execution Acoustically





"RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis"
Genkin et al., http://www.tau.ac.il/~tromer/acoustic/

LADS: Protecting EMSDs via Analog Sensing



- Explore different emission modalities
  - e.g., EM, acoustic, power
- Combine multiple modalities
- Many-to-one, many-to-many tracking

LADS Program Structure

TA1: Protecting Embedded and Mission-Specific Devices (EMSDs) via Analog Sensing

- ***Goal:*** Develop new cyber techniques in digital devices by monitoring the analog emissions across different/multiple modalities:
  - Tracking fidelity vs. device complexity
  - Fidelity: Known/unknown code, control flow tracking, instruction tracking, …

Parameters/Challenges:
- **Distance**
- **Polarization**
- **Multipath**
- **Ambient Noise**

- ***Output*****:** Monitoring devices; network architectures; algorithms for mapping digital artifacts to analog emissions

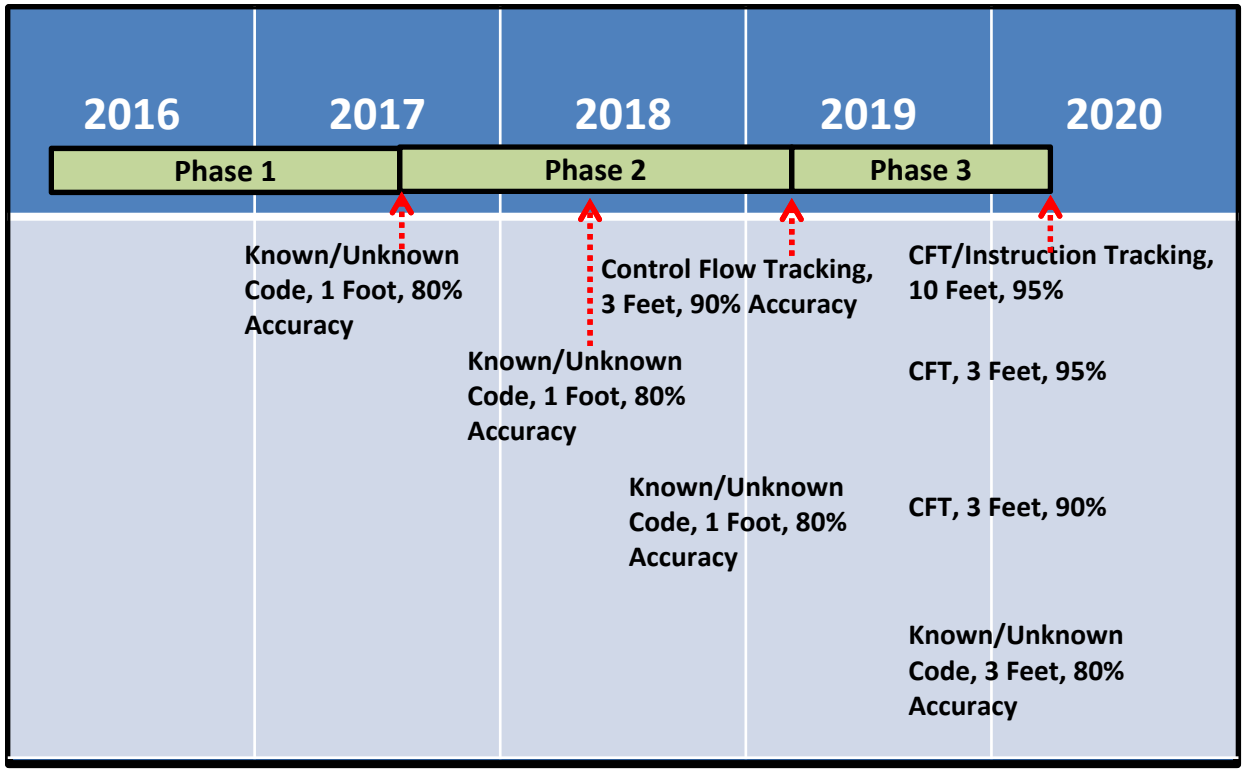
- ***Methodology:***
  - Identify and quantify useful analog signals
    - Develop predictive models
  - Map device firmware, configuration, and data to cyber-relevant analog emissions model
    - Unknown firmware & configuration
  - Boost signal via software and/or analog component modifications
- Reconcile tracked device emissions with emissions model
- Cooperative sensing and tracking

TA1 Program Metrics

- Measure effectiveness as a ROC curve (detection vs. misdetection) on devices of increasing complexity
  - Fidelity: Known/unknown code, control flow tracking, instruction tracking, others
  - Secondary characteristics depending on modality, e.g., distance, polarization
- Phase 1 Program Metrics:
  - Demonstrate feasibility of discriminating between known/unknown code executing on a simple IoT-type device
    - 80% accuracy or higher, assuming knowledge of the firmware
    - Close proximity (signal level of 3dBi or less at 1 foot), in an environment with low ambient noise (Demonstration at Month 18)
  - Demonstrate the impact of modifying the software executing on the device to boost detection of software/firmware compromise
- Phase 2 Program Metrics:
  - Demonstrate the ability to correctly identify with 80% accuracy, at close proximity (1 foot), from among several instances of known code/unknown code, while improving accuracy (90%) and distance (3 feet or more) for the simpler devices
    - FPGA board by M30, thin-client computer or simple “feature phone” cell phone by M36
    - Demonstrate the techniques for devices of increasing complexity
- Phase 3 Program Metrics:
  - Extend the techniques for more complex devices (e.g., a high-end smartphone or laptop) while increasing accuracy, fidelity, and discriminating capability for the devices examined in earlier phases
    - Improve accuracy to 95% with close proximity to 10 feet (Demonstration at M48)

Program Schedule and Progress Metrics

Primary Metrics:
- **Fidelity**
- **Distance**
- **Accuracy**



Evaluation Details

- Each performer conducts own evaluation for each milestone
  - Provide data and prototypes to DARPA and AFRL to conduct independent validation
  - Government reserves the right to engage third parties to independently validate results

- Each performer responsible for specifying in their proposal which devices they will use, for each of the four device classes
  - Make your choices based on proposed sensing modalities
  - Avoid selection of Government-/DoD-specific equipment
  - Suggestion: Specify groups of devices in each class
    - Government may choose to limit to a subset, or propose substitute devices during contract negotiations

Meetings and Reporting Requirements

- Two Annual Principal Investigator (PI) Meetings
- Quarterly Technical Reviews between PI Meetings
- Monthly Progress Reports
  - Technical Report describing progress, resources expended and issues requiring Government attention, provided 10 days after the end of each month
- Financial/Technical Progress Reporting to the DARPA Technology Financial Information Management System (TFIMS)
- Software Development Plan
- Final Technical Report
- Agent: AFRL/RYMH

Funding and Programmatic Details

- Proposals due: Tuesday, November 10 at noon ET
- Government anticipates multiple awards
  - Procurement Contract or Other Transaction
- Proposers to TA1 are not required to hold or obtain security clearances
- Proposers to TA1 do not require access to the LADS Classified Addendum
- Organizations can submit separate proposals to all Technical Areas
  - Which to consider for award is at the discretion of the Government
- To expedite award contracting, proposers are encouraged to have sub-award agreements in place ahead of award notification